IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF PUERTO RICO

UNITED STATES OF AMERICA Plaintiff, v. MIGUEL GONZÁLEZ-AROCHO, Defendant.	CRIMINAL NO.: 22-418 (PAD)

REPORT & RECOMMENDATION

I. PROCEDURAL BACKGROUND

On September 28, 2022, a grand jury returned an indictment against Miguel González-Arocho ("Defendant") charging him with possession and receipt of child exploitation material in violation of 18 U.S.C. § 2552(a)(4)(B), (a)(2). ECF No. 3. Pending before the court is Defendant's motion to suppress to which the United States of America ("the Government") subsequently filed a response in opposition. ECF Nos. 34, 38. Thereafter, Defendant replied, and the Government filed a sur reply. ECF Nos. 41, 44. Defendant seeks to suppress the contents found within his Apple iPhone 13 Pro Max with the International Mobile Equipment Identity ("IMEI") number 352114952598152 (the "iPhone 13"), arguing his Fourth Amendment right was violated. ECF No. 34 at 6.[1] A suppression hearing was held on January 10, 2024. ECF No. 51. For the reasons set forth below, Defendant's motion to suppress should be DENIED.

[1] An IMEI is a unique number assigned to each cellular phone. For example, if an individual changes cellular device, the new phone would have a different IMEI compared to the old phone. Hr'g, January 10, 2024, at 1:53 p.m., 2:23–2:24 p.m.

II. FACTUAL BACKGROUND

During October 2021, Homeland Security Investigations ("HSI") Puerto Rico received a referral from HSI Phoenix concerning phone numbers associated with Puerto Rico engaging in online chat rooms using the Viber application to distribute child pornography. One of those phone numbers was (787) 413-7611, Defendant's phone number, which HSI later determined was registered to T-Mobile. Subsequently, HSI Task Force Agent Albert Villanueva López ("TFA Villanueva") served summons to T-Mobile requesting information associated with phone number (787) 413-7611. T-Mobile produced a report (ECF No. 52-1) on April 30, 2022, providing, among other things, that the phone number was registered to Defendant and had been since December 2015, a residential address that was later determined to be Defendant's sister's, and that the phone was an iPhone 6S with the IMEI 353316071131711 (the "iPhone 6S").[2] Hr'g, January 10, 2024, at 10:23–10:30 a.m., 10:32 a.m.

Armed with this information, HSI verified the information provided by T-Mobile with the databases of the Department of Motor Vehicles ("DAVID") and Department of Treasury. DAVID confirmed Defendant's identity, provided the address of his residence, and noted that Defendant had two vehicles registered under his name. HSI then conducted surveillance of Defendant's residence where TFA Villanueva observed Defendant driving both vehicles to and from his residence. Next, TFA Villanueva submitted a search warrant application to search the iPhone 6S, explicitly noting that "[t]he property to be searched is **Apple iPhone 6S 64GB IMEI: 353316071131711** with number (787) 413-7611 . . . , belonging to or being used by **Miguel GONZ[Á]LEZ-Arocho**." ECF No. 52-2 at 2. The court issued said warrant on May 11, 2022,

[2] While the report does not explicitly state that the phone was an Apple iPhone 6S, TFA Villanueva testified that the IMEI and Subscriber Identity Module ("SIM") numbers provided in the report identified the model of Defendant's phone. Hr'g, January 10, 2024, at 10:27 a.m.

authorizing the search of the iPhone 6S for evidence relating to child pornography. ECF No. 52-4 at 1, 3–4; Hr'g, January 10, 2024, at 10:30–10:34 a.m.

Not long before 10:00 a.m. on May 18, 2022, TFA Villanueva and other agents initiated the execution of the search warrant by conducting a surveillance of Defendant's residence. As agents observed Defendant enter his vehicle near the Residence, they intercepted him. During this initial interaction, agents identified Defendant, and TFA Villanueva seized the iPhone 13 that was on his person, not the iPhone 6S listed in the search warrant.[3] Defendant then accompanied TFA Villanueva and Agent Alek Pacheco ("Agent Pacheco") into a government vehicle to conduct an interview, which was recorded. *See* Exhibit 5; Hr'g, January 10, 2024, at 10:39–10:42 a.m.

During the interview, TFA Villanueva sat in the vehicle's front-passenger side while Defendant, who was not restrained, and Agent Pacheco sat in the back. Before initiating questioning, Agent Pacheco explained he had a search warrant for an Apple iPhone with Defendant's cell phone number; gave Defendant a copy of the warrant, which Defendant examined; and explained the terms of the warrant while Defendant looked at it. *See* Exhibit 5, at 2:00–2:18, 3:45–4:45; ECF No. 52-5 at 3. Immediately after, Agent Pacheco administered *Miranda* rights to Defendant and executed a *Miranda* form (ECF Nos. 52-6–7) to which Defendant signed and indicated that he was willing to speak to police officers. Exhibit 5, at 4:45–6:40. As the interview continued, Defendant proceeded to give the passcode of the iPhone 13 and credentials to access various social media applications on his phone, including his Viber account. *See e.g.,* Exhibit 5, at 7:40, 16:30; ECF No. 52-5 at 8, 19–21. Additionally, during the interview,

[3] TFA Villanueva testified that after seizing the iPhone 13, he handed it to HSI's forensic team. Hr'g, January 10, 2024, at 10:40 a.m. However, in the video recording of Defendant's interview that followed the initial intervention, TFA Villanueva is seen in possession of the iPhone. Exhibit 5, at 16:40.

Defendant signed a consent form to search his residence (ECF Nos. 52-8–9) and a consent form to conduct a forensic search of his laptop computer and external hard drive inside of the residence (ECF Nos. 52-10–11). *See* Exhibit 5, at 29:50–30:30. After the interview, agents seized Defendant's laptop computer and external hard drive from his residence. On May 18, 2022, the same day the warrant was executed, TFA Villanueva completed a search warrant return noting that the iPhone 13 with phone number (787) 413-7611 was seized. ECF No. 52-12 at 2. HSI forensics later conducted a forensic search of the iPhone 13, laptop, and external hard drive. A forensics report was produced on July 19, 2019, noting that only the iPhone 13 contained incriminating evidence relating to child pornography. ECF No. 52-13 at 1–4; Hr'g, January 10, 2024, at 11:01 a.m., 11:47–11:53 a.m.

III. ANALYSIS

Defendant argues that HSI did not have a warrant to search his phone because the search warrant was for the iPhone 6S, not the iPhone 13 that was searched. ECF No. 34 at 3–4. Additionally, Defendant contends that HSI did not act pursuant to any exception of the warrant requirement. ECF No. 41 at 3, 6. The Government opposes, arguing that the warrant covered the iPhone 13, and in the alternate, two exceptions to the warrant requirement apply: consent and good faith.

A. Whether the warrant authorized the search of the iPhone 13.

The United States contends that its warrant authorized the search of the iPhone 13 even though the search warrant explicitly noted that it was for an iPhone 6S. ECF No. 44 at 1. This issue can be reduced to the whether the iPhone 6S listed in the warrant is—for purposes of the essence of what is being searched—the same as the iPhone 13 that was actually searched. At first glance the obvious answer would be no because the two devices are two distinct iPhone models

with different IMEIs and, to some extent, features or capabilities. Furthermore, as Defendant argues, in issuing the search warrant, the court made a probable cause determination as to the iPhone 6S, not the iPhone 13, and nothing prevented HSI from securing another warrant for the iPhone 13 once it realized the iPhone 13 was not the phone model explicitly listed in the search warrant.

On the other hand, to some degree these phones are substantially the same—if not in terms of their appearance, at least in terms of their content—because they are both iPhones owned by the same person with the same phone number, and it is reasonably common for individuals to transfer data between an old and new phone when they upgrade. *E.g., Coyne v. Los Alamos Nat'l Sec., LLC*, No. 15-CV-54, 2017 WL 3225466, at *9 (D.N.M. May 1, 2017) ("[T]he Court agrees with Defendants that it is common for a person to transfer data from an old phone onto a new phone."); *see also Lamb v. Liberty Univ.*, No. 6:21-CV-00055, 2022 WL 3692670, at *5 (W.D. Va. Aug. 25, 2022) ("It is also unusual for a person to exchange phones without transferring data from the old phone onto the new."). With those similarities in mind, one could argue that a cell phone is a container of data, uniquely identified by its phone number. Because the court determined that there was probable cause to search the iPhone 6S with the phone number (787) 413-7611 belonging to Defendant, it was rational to extend that search to the iPhone 13 with phone number (787) 413-7611 belonging to Defendant because the iPhone 13 was reasonably related to the iPhone 6S listed in the search warrant. *Cf. United States v. Gentry*, 642 F.2d 385, 387 (10th Cir. 1981) ("When a logical nexus exists between seized but unnamed items and those items listed in the warrant, the unnamed items are admissible."); *United States v. Gomez-Soto*, 723 F.2d 649, 655 (9th Cir. 1984) ("The failure of the warrant to anticipate the precise container in which the material sought might be found is not fatal.").

However, the Supreme Court has made clear that there is a "general preference to provide clear guidance to law enforcement through categorical rules. . . . not in an ad hoc, case-by-case" basis. *Riley v. California*, 573 U.S. 373, 398 (2014). A ruling finding this search warrant valid to cover the iPhone 13 is in tension with said principle and would possibly create more questions than answers. Put differently, finding this search warrant valid would require a workable test that law enforcement agents would have to employ to determine which two devices are similar enough to be covered under the same warrant. Evidently, this "test would launch courts on a difficult line-drawing expedition to determine which" electronic devices are sufficiently alike to be covered under the same warrant. *Id.* at 401. Furthermore, this test would need to be constantly adjusted to avoid becoming obsolete due to the rapid changes in technology. For example, what if different devices such as an iPhone, iPad, and iWatch all respond to the same phone number? Would the search warrant for the phone apply equally to a tablet and a watch simply because they share a cellphone's number and are synchronized or interconnected or share the same cloud storage with the cellphone?[4] The presentation of the Government's evidence at the suppression hearing leaves these questions unanswered.

B. Whether Defendant's consent to search his phone was valid.

The Government argues that the search of the iPhone 13 was valid because Defendant consented to the search of that phone. ECF No. 38 at 4. A defendant may waive his rights under the Fourth Amendment by voluntary consent to a search. *Davis v. United States*, 328 U.S. 582, 593–94 (1946). "Consent is voluntary if it is 'the product of an essentially free and unconstrained

[4] It would also not have been an onerous burden on the Government, once the agents realized that the seized phone was not an iPhone 6S, to seek a new or amended search warrant. As discussed below, although it is possible that the agents did not realize at the moment of the seizure of the phone that the device that Defendant had was an iPhone 13 and not an iPhone 6S, the search warrant's return evidences that at some point in time on the very same day that the execution of the warrant took place, TFA Villanueva became aware that the seized phone was an iPhone 13 and not an iPhone 6S.

choice.'" *United States v. Chhien*, 266 F.3d 1, 7 (1st Cir. 2001) (quoting *Schneckloth v. Bustamonte*, 412 U.S. 218, 225 (1973)). In determining voluntariness, the focus is often on whether the individual's will has been overborne and his capacity for self-determination critically impaired. *See Schneckloth*, 412 U.S. at 225; *United States v. Calderon*, 77 F.3d 6, 9 (1st Cir. 1996). However, before reaching the question of whether a consent was voluntary, the Government must show that there was in fact consent, which "may be in the form of words, gesture, or conduct." *United States v. Griffin*, 530 F.2d 739 (7th Cir. 1976) (citing *Robbins v. MacKenzie*, 364 F.2d 45, 48–49 (1st Cir. 1966)). "Consent to a search need not be express [and] may be fairly inferred from context." *Birchfield v. North Dakota*, 579 U.S. 438, 476 (2016).

First, the Government points to a consent form (ECF Nos. 52-10; 52-11) signed by Defendant authorizing HSI agents to seize and search electronic equipment. Viewed in isolation, this form could be construed as allowing the search of the iPhone 13 because it explicitly lists "cellular telephones" among the items to be searched. ECF No. 52-11. However, TFA Villanueva's testimony clearly articulated that this consent form was only to authorize the search of those items found at the Defendant's residence (as opposed to his person), namely Defendant's laptop computer and external hard drive, both of which were seized inside his residence after he was interviewed and after the iPhone 13 was seized:

> Q. [Defense Counsel] The purpose of Exhibit 8 [ECF Nos. 52-10; 52-11] was to memorialize [Defendant's] consent to the search and seizure of his computer and his hard drive, right?
>
> A [TFA Villanueva] . . . This is like a consent but for the . . . forensic agents of the computer and the . . . hard d[rive].
>
> Q. So this is for the hard d[rive] and the computer?
>
> A. Yes.

> Q. The iPhone [13], the cell phone, was not covered by that consent because it had already been seized?
>
> A. No, it was seized. This was for the other items inside his home.

Hr'g, January 10, 2024, at 2:07–2:08 p.m. Therefore, this specific consent form cannot be basis for valid consent of the iPhone 13 because it was meant for matters found in his residence.

Second, the Government points to Defendant's actions and words during his interview with Agent Pacheco and TFA Villanueva to suggest he consented to the search of the iPhone 13. The threshold inquiry is whether these actions and words, taken in the context they were given, adequately demonstrate consent that authorized the iPhone 13's forensic search that later ensued. The measure of the scope of a Defendant's consent is a test of objective reasonableness: "what would the typical reasonable person have understood by the exchange between the officer and the [defendant]?" *Florida v. Jimeno*, 500 U.S. 248, 251 (1991). "Typically, courts look beyond the formal wording of the consent itself to the totality of the circumstances that inform the meaning of those words in a given situation, which can encompass "contemporaneous police statements and actions." *United States v. Stierhoff*, 549 F.3d 19, 23–24 (1st Cir. 2008) (citation omitted)).

Before addressing whether Defendant consented to the search of the iPhone 13, it should be noted that at the beginning of the interview when Agent Pacheco tells Defendant he has a warrant, Agent Pacheco can only be heard saying the search warrant "is for an Apple iPhone, with telephone number" (787) 413, not the complete number of (787) 413-7611. ECF No. 52-5 at 3; Exhibit 5, at 2:10–2:20. This is because once Agent Pacheco finishes saying the sixth number of Defendant's cell phone number, Defendant immediately interrupts him; however, it is unclear what Defendant said exactly. Because Agent Pacheco responds to Defendant's interruption with "okay" and continues the interview, a reasonable inference can be drawn that Defendant either

stated the last four digits of his phone number or said something to confirm Agent Pacheco had the correct phone number. To dispel any possible doubt about whether the interviewing agents and Defendant were on the same page about Defendant's phone number, Defendant can be heard stating his phone number to the agents later during the interview. Exhibit 5, at 17:48; ECF No. 52-5 at 20–21.

Here, before starting the interview, TFA Villanueva had already seized Defendant's phone and had it in his possession. The interview began with Agent Pacheco explaining to Defendant that he had a search warrant for an Apple iPhone with phone number (787) 413-7611 and that Defendant was being investigated concerning matters related to "crimes against children." Exhibit 5, at 2:00; ECF No. 52-5 at 3–4. As the interview progressed, Defendant provided information to help agents access the phone. Defendant first provided the iPhone 13's passcode. Exhibit 5, at 7:40; ECF No. 52-5 at 8. Next, Defendant provided his Viber account credentials, which Agent Pacheco used to access the account beside Defendant during the interview. Exhibit 5, at 16:30; ECF No. 52-5 at 19–21. After attempting to access Defendant's Viber account, Agent Pacheco, in Defendant's presence, stated: "We must see the . . . forensic and see what they can pull." Exhibit 5, at 21:55; ECF No. 52-5 at 25. Afterward, Agent Pacheco reiterated that the iPhone 13 would be going to a lab for forensics analysis after the interview. Exhibit 5, at 34:58; ECF No. 52-5 at 40. Defendant subsequently provided the agents with his credentials for Facebook and acknowledged that he had an Instagram account, indicating that the agents could check that as well. Exhibit 5, at 38:44–40:12; ECF No. 52-5 45–47.

Defendant's actions and words detailed above—taken in the context that he knew what he was being investigated for and that HSI already possessed his phone—are enough to demonstrate approval to search his phone. While the agents had the iPhone 13 in their

possession, Defendant provided the passcode and credentials to several social media platforms, displaying no hesitation with agents going through his phone. Indeed, Defendant witnessed Agent Pacheco download and log into his Viber account, the account that Defendant and the agents knew was the focal point of the investigation. *Cf. United States v. Thurman*, 889 F.3d 356, 368 (7th Cir. 2018) ("Because it was clear that the agents were investigating Mr. Thurman's recent drug sales, a reasonable person in his position would expect them to [conduct a *forensic*] search [of] the phone for relevant deleted messages.").

The final question is whether Defendant's consent was voluntary. In this regard, Defendant argues that it was not because of the Supreme Court's decision in *Bumper v. North Carolina*, 391 U.S. 543 (1968). In *Bumper*, the prosecution sought to justify the search of a house on the sole basis of the owner's consent. The owner, however, consented only after a police officer stated that he had a warrant to search the house. The Supreme Court held that the officer's statement rendered the consent invalid:

> When a law enforcement officer claims authority to search a home under a warrant, he announces in effect that the occupant has no right to resist the search. The situation is instinct with coercion—albeit colorably lawful coercion. Where there is coercion there cannot be consent.

Id. at 550. However, "assertion of authority is one factor, not the only factor, in considering whether consent was voluntary." *United States v. Parrish*, 942 F.3d 289, 294 (6th Cir. 2019) (citation omitted); *see also Schneckloth v. Bustamonte*, 412 U.S. 218, 226 (1973) (holding that *Bumper* renders consent invalid only "if under all the circumstances it has appeared that the consent was not given voluntarily—that it was . . . granted *only* in submission to a claim of lawful authority." (emphasis added)). Therefore, the Supreme Court in *Schneckloth* declined to make a per se rule that any time officers make a claim of lawful authority, the consent that follows is always involuntary. Citing *Bumper*, Defendant argues that he could not refuse the

search of the iPhone 13 because Agent Pacheco falsely and knowingly represented that HSI had a warrant for Defendant's Apple iPhone with the phone number (787) 413-7611. ECF No. 41 at 4–5. In other words, Defendant argues that Agent Pacheco deceitfully misrepresented the warrant by not explicitly telling Defendant that it was for the iPhone 6S. This argument cannot flourish.

First, Agent Pacheco's representation was not a deceptive claim of authority. Not all claims of authority given by police are the same. A claim of lawful authority knowing it is false cannot be equated to such being honestly mistaken about its inaccuracy. When a false claim of authority is made knowingly, consent is strongly presumed to be invalid.[5] *See United States v. Vazquez*, 724 F.3d 15, 22 (1st Cir. 2013) ("The law is clear . . . that consent to a search is invalid if given only because of an officer's knowingly false assurance that there will soon be a lawful search anyway." (citations omitted)); *Pagán-González v. Moreno*, 919 F.3d 582, 596 (1st Cir. 2019) ("[C]ourts have uniformly recognized that the Fourth Amendment *may* be violated when consent is obtained through a law enforcement officer's false claim of authority . . . . In such instances, the deception *may* be sufficient on its own to vitiate the voluntariness of the resulting 'consent.'" (emphasis added)).

While Agent Pacheco did not explicitly state that HSI had a search warrant for a model 6S iPhone, before commencing any questioning Agent Pacheco provided Defendant with a copy of the search warrant and briefly explained some aspects of the warrant while Defendant was examining it. Exhibit 5, at 3:53–4:50. Before handing Defendant a copy of the warrant, Agent Pacheco turned on a light directly above Defendant to ensure Defendant could see the contents of the warrant. Exhibit 5, at 3:26. Additionally, while alluding to the warrant, Agent Pacheco is

[5] At least one other circuit has suggested that a knowingly false claim of authority will automatically render consent invalid. *Hadley v. Williams*, 368 F.3d 747, 749 (7th Cir. 2004) (stating that consent was "vitiated not only by the claim of the police to have a warrant ... but also by fraud," and explaining that the consent "was procured by an outright and material lie [that the police had a warrant], and was therefore ineffectual")

seen in the video recording pointing to the warrant, which Defendant is holding in his hands and examining. Exhibit 5, at 3:53–4:03, 4:32–4:38. In light of these circumstances, it is not evident that Agent Pacheco omitted that the warrant was for an iPhone 6S because he was knowingly trying to deceive Defendant. It is more plausible that the agents had simply not realized at the moment that the iPhone seized, despite answering to the same target phone number, was a different model. Therefore, Agent Pacheco's representation of the warrant was not knowingly false; instead, it was made in his honest belief that HSI had a valid warrant.

Even though Agent Pacheco's claim of authority was not made in bad faith, it is still a factor that weighs against a finding of voluntary consent. As previously noted, a claim for lawful authority is only one factor in the voluntariness analysis. "Whether consent was voluntary or the result of coercion is a question of fact to be determined from an examination of the totality of circumstances." *United States v. Marshall*, 348 F.3d 281, 286 (1st Cir. 2003) (citing *United States v. Twomey*, 884 F.2d 46, 51 (1st Cir. 1989)). "Factors to be considered include [but are not limited to] age, education, experience, knowledge of the right to withhold consent, and evidence of coercive tactics." *Id.* (citation omitted).

Here, the following facts weigh in favor of voluntary consent: Defendant was told he was not under arrest, Defendant was read his *Miranda* rights and voluntarily waived them, Defendant was not restrained during the interview, the officers talked calmly to Defendant during the interview, the interviewing officers did not have their weapons drawn during the interview, Defendant appeared calm during the interview, the interview was conducted during the day near Defendant's home, Defendant was offered water during the interview, and Defendant was a full-time student in college studying engineering with 15 years of experience in banking and

experience working as manager at a dealership. *See* Exhibit 5 (DVD); ECF No. 52-5. Nothing in the recorded interview suggests that Defendant was not able to understand what was going on.

On the contrary, the following facts weigh against voluntary consent: Defendant was not explicitly told that despite the search warrant already shown to him he had a right not to consent to the search of the iPhone 13, agents already had the iPhone 13 in their possession before Defendant began sharing passwords and access-related information, and there were additional agents near the government vehicle where the interview was being conducted.

Although an argument could be made that because the Defendant conveyed his cellphone passcode and Viber account credentials only after he waived his *Miranda* rights, and these authorizations came after Defendant knew that he did not have to speak to the agents, it follows that Defendant knew he did not have to provide consent in the form of sharing the iPhone 13 passcode and social media account credentials. *Cf. United States v. Orlandella*, No. CR 19-10010, 2022 WL 17852423, at *6 (D. Mass. Dec. 22, 2022) ("[T]he defendant understood that he did not have to speak to the agents and voluntarily agreed to do so. The court finds that the corollary of this is that the defendant knew he did not have to consent to a search of his car."). However, cases such as *Orlandella* are inapposite to the circumstances at bar because *Orlandella* involved a warrantless search of a car. In the case presently before the court, however, Defendant waived his *Miranda* rights after he was told that the agents had a search warrant for his phone which the agents already had in their possession while he was sitting inside the agents' car. It would not have been far-fetched for Defendant to believe that in light of the search warrant, refusing consent to search the phone was pointless. Moreover, the voluntariness of consent is severely diminished when law enforcement already has access to the object to be searched. *See Robbins v. MacKenzie*, 364 F.2d 45 (1st Cir. 1966) (stating "that courts should be skeptical of a

purported consent to a search made after the officer had been admitted" inside the home and listing cases from other circuits); *United States v. Lewis*, 274 F. Supp. 184, 188 (S.D.N.Y. 1967) (holding consent involuntary where, among other things, defendant's apartment keys had already been taken by officers, thereby indicating that the officers were going to search defendant's apartment if they could locate it). Accordingly, Defendant's consent to the search of his phone was not voluntary and therefore invalid.

C. Whether the good faith exception applies.

Finally, the Government argues that the good faith exception applies. "The usual remedy for seizures made without probable cause is to exclude the evidence wrongfully seized in order to deter future violations of the Fourth Amendment." *United States v. Brunette*, 256 F.3d 14, 19 (1st Cir. 2001) (citation omitted). However, the exclusionary rule is inapplicable under the good faith exception "where an objectively reasonable law enforcement officer relied in good faith on a defective warrant because suppression in that instance would serve no deterrent purpose." *Id.* (citing *United States v. Leon*, 468 U.S. 897, 920–21 (1984)). "The Government bears the burden of showing that the police officers acted with objective good faith, . . . [evaluating] all of the attendant circumstances at the time of the warrant application and its execution." *Id.* at 17.

Here, the application of the search warrant was made in good faith. Nothing in the record suggest that the agents acted recklessly or falsely in the application for the search warrant. To the contrary, TFA Villanueva's actions leading up to the execution of the search warrant show he acted with diligence. Soon after Defendant's phone number was linked to the Viber chat distributing child pornography, TFA Villanueva served summons on T-Mobile to acquire more information regarding the phone and its subscriber. Thereafter, HSI cross-referenced the information from the T-Mobile summons with records from the Departments of Motor Vehicles

and Treasury to subsequently conduct surveillance of Defendant and ensure HSI had identified the right person. Only then did TFA Villanueva apply for a search warrant, detailing the information he had available to him regarding the phone to ensure he complied with the requirement for particularity. Therefore, TFA Villanueva's actions in the application of the warrant were made in good faith. Hr'g, January 10, 2024, at 10:23–10:34 a.m.

The parties dispute whether HSI acted in good faith during the execution of the search warrant. Ultimately, there are two ways that good faith would apply toward the execution of the search warrant in this case. The first being that the agents reasonably did not know that they had the wrong phone before the forensic search was conducted. The second is that although agents knew they did not have the exact phone listed in the search warrant, they had an objectively reasonable belief that the warrant authorized them to conduct a search of the iPhone 13.

The evidence shows that the first way of proving good faith is inapplicable here because HSI knew that it had seized the iPhone 13, rather than the iPhone 6S listed in the search warrant, before the iPhone 13 was subject to a thorough forensic search. HSI knew it seized an Apple iPhone 13, not the iPhone 6S, on the same day the phone was seized from Defendant. This conclusion is evident by the search warrant return dated the same day as the execution of the search warrant, May 18, 2022, which explicitly notes that an iPhone 13, not an iPhone 6S, was seized. ECF No. 52-12 at 2.[6] Therefore, the Government cannot claim that the forensics team that searched the phone was under the impression that they were searching an iPhone 6S, rather than an iPhone 13.

[6] Despite being dated July 19, 2022, the forensic report detailing the iPhone 13's forensic search inaccurately notes that Defendant's electronic devices, including the iPhone 13, were submitted for forensic examination on January 27, 2022, a date before the execution of the search warrant when the phone was seized. ECF No. 52-13 at 2.

However, the agents acted in good faith during the execution of the warrant because they reasonably believed the warrant authorized them to search the iPhone 13. As discussed above, whether the search warrant issued in this case duly authorized the search of an upgraded phone is an inquiry that does not necessarily have a straightforward answer. TFA Villanueva explained that his investigation from the onset was focused on Defendant's phone number, not on a specific device. Hr'g, January 10, 2024, at 10:33 a.m. Indeed, the phone number was the genesis of HSI's investigation; it notified HSI that it was a number associated to Puerto Rico; it was linked to the Viber chat that distributed child pornography; it led HSI to seek more information from T-Mobile regarding the subscriber and the characteristics of the physical device; it was registered to Defendant since 2015; and it ultimately was assigned to the device that was seized. ECF No. 52-1 at 1; Hr'g, January 10, 2024, at 10:23–10:30 a.m. It was also reasonable for HSI to assume that Defendant had upgraded his phone when T-Mobile reported he had the iPhone 6S, and it was later found that he had the iPhone 13, especially where the phone was the same brand, had the same number, and belonged to the same person. Additionally, as explained above, it is commonly known that individuals transfer the data of their phones when they upgrade their phones. Therefore, it was not in bad faith that the agents, even though they knew they did not have the iPhone 6S listed in the search warrant, believed that the search warrant authorizing the search of the content of the iPhone 6S one week before its execution would be equally applicable to the same content transferred to an upgraded iPhone 13 with the same phone number and in the possession of the same person owning and/or using the iPhone 6S.

Defendant argues that the agents did not act in good faith during the execution of the search warrant because they did not independently verify that they had the right phone with the right number, other than Defendant's own verbal confirmation. Hr'g, January 10, 2024, at 3:20

p.m. During the suppression hearing, TFA Villanueva testified that he did not call the cell phone to verify it had the number listed in the warrant, presumably because he took Defendant's word for it. *See* Hr'g, January 10, 2024, at 2:10–2:11 p.m. While calling the phone himself would have provided TFA Villanueva with further assurance, it was reasonable that he took Defendant's word as true. At this point in time, TFA Villanueva had been running surveillance of Defendant and had reason to believe that he was in possession of a phone with a phone number that was linked to the distribution of child pornography. It was also reasonable for him and Agent Pacheco to take Defendant's word as true because Defendant's statement confirming as correct the target phone number listed in the warrant was against his own interest and could subject him to criminal liability. *Cf. Williamson v. United States*, 512 U.S. 594, 594 (1994) ("[Federal Rule of Evidence 804(b)(3) is founded on the commonsense notion that reasonable people, even those who are not especially honest, tend not to make self-inculpatory statements unless they believe them to be true."). If anything, Defendant had an incentive to deny the phone number belonged to him to distance himself from any investigation the agents were conducting regarding a device with the number explicitly stated on the face of the search warrant. Therefore, the fact that TFA Villanueva did not take additional measures to verify the iPhone 13 had the phone number listed in the warrant does not negate HSI's good faith execution of the search warrant. In sum, regardless of whether the search warrant validly encompassed the seized iPhone 13, HSI acted in good faith during both the application and the execution of the warrant, and therefore it is recommended that the contents of the iPhone 13 not be suppressed.

IV. CONCLUSION

For the foregoing reasons, Defendant's motion to suppress (ECF No. 34) should be DENIED. Accordingly, the contents of Defendant's phone should not be suppressed. The parties

have fourteen (14) days to file any objections to this report and recommendation unless otherwise ordered by the court. Failure to file the same within the specified time waives the right to object to this report and recommendation. Fed. R. Civ. P. 72(b)(2); Fed. R. Civ. P. 6(c)(1)(B); D.P.R. Civ. R. 72(d); *see also* 28 U.S.C. § 636(b)(1); *Henley Drilling Co. v. McGee*, 36 F.3d 143, 150–51 (1st Cir. 1994); *United States v. Valencia*, 792 F.2d 4 (1st Cir. 1986).

IT IS SO RECOMMENDED.

In San Juan, Puerto Rico, this 25th day of January, 2024.

s/Marcos E. López
U.S. Magistrate Judge